Zbornica računovodskih servisov

Gospodarska zbornica Slovenije

Dimičeva 13 ■ 1504 Ljubljana ■ T: (01) 58 98 316 ■ F: (01) 58 98 100 ■ zrs@gzs.si ■ www.gzs.si/zrs

Ponudba članom ZRS
za izvedbo varnostnega pregleda ter odkrivanja ranljivosti

Potek izvedbe storitev

Za izvedbo napadov na daljavo se ustvari nova navidezna digitalna identiteta.

Na podlagi pridobljenih informacij se začne izvajati ciljane napade na daljavo. Ti vključujejo:

1. Pošiljanje navidezno zlonamerne elektronske pošte na tiste naslove, ki so bili pridobljeni v prvi fazi.
    - Elektronska pošta z navidezno zlonamerno priponko.
    - Elektronska pošta s povezavo na klonirano spletno stran podjetja ki je namenjena odtujitvi uporabniškega imena in gesla zaposlenega (Phishing).
2. Izvajanje telefonskih klicev.

Ad 1.) Pošiljanje navidezno zlonamerne povezave

Večina novodobnih vdorov targetira končnega uporabnika, saj je ta postal najšibkejši člen v celotni varnostni verigi. Spletni napadalci iz prosto dostopnih virov ugotovijo elektronske naslove vašega podjetja in vašim zaposleni pošiljajo zlonamerna elektronska sporočila. Pri storitvi PRO.red se tudi sami postavijo v vlogo napadalca in izvajajo navidezno škodljive aktivnosti v popolnem sodelovanju z naročnikom.
Izbranim uporabnikom, katerih elektronske naslove so pridobili na internetu, pošljejo sporočilo, ki vsebuje navidezno zlonamerno datoteko. Ob zagonu datoteke se izvede kontrolirana programska koda, ki se poveže z računalnikom izvajalca in na ta način lahko prevzamejo nadzor nad končnim uporabnikom.
V kolikor tekom pregleda ugotovijo, da ima organizacija ustrezno implementirane varnostne mehanizme in priponka končnega uporabnika ne doseže preko elektronske pošte, uporabniku pošljejo elektronsko sporočilo z navidezno zlonamerno povezavo. Ta so razdeljena v dve kategoriji:
1. V elektronskem sporočilu se nahaja povezava, katera ob kliku izvede prenos zlonamerne datoteke na žrtvino napravo.
2. V elektronskem sporočilu se nahaja povezava, katera ob kliku uporabnika pelje na kopirano spletno stran podjetja (angl. clone). Spletna stran se ne nahaja na pravi domeni podjetja, ampak se za namene testiranja registrira novo domeno in uporabnika z metodami socialnega inženiringa prepriča, da v to spletno stran vpiše uporabniško ime in geslo. V kolikor so pri tem uspešni, so pridobili domenskega uporabnika vašega podjetja.

Ad 2.) Izvajanje telefonskih klicev

Pri izvajanju telefonskih klicev gre za to, da iz prosto dostopnih informacij pridobijo telefonsko številko zaposlenega in izvedejo podrobnejšo raziskavo. Raziskava

vključuje pregled:

- Socialnih omrežij zaposlenega (LinkedIn, Facebook, …)
- Interesnih skupin zaposlenega
- Hobijev in ciljev
- Službenih razmerij in zadolžitev

Ko pridobijo zadostno količino informacij, s katero predpostavljajo, da bi lahko zavedli zaposlenega, vzpostavijo z njim stik preko telefonskega klica. Predstavijo se kot zaupanja vredna oseba, npr. njegov zaposleni, vodja informatike ali drugi, in od njega poizkušajo pridobiti domensko uporabniško ime in geslo. V kolikor pri tem niso uspešni, zaposlenega usmerjamo v akcije na računalniku, ki vodijo bodisi do prenosa in zagona zlonamerne kode iz interneta, bodisi do spremembe.